501P0364US00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　８月２９日

出願番号
Application Number: 特願２０００－２６４５０６

願人
Applicant(s): ソニー株式会社

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　0000613105
【提出日】　平成12年 8月23日
【あて先】　特許庁長官殿
【国際特許分類】　H04K 1/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　市村　元
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100086841
【弁理士】
【氏名又は名称】　脇　篤夫
【代理人】
【識別番号】　100114122
【弁理士】
【氏名又は名称】　鈴木　伸夫
【先の出願に基づく優先権主張】
【出願番号】　特願2000- 76373
【出願日】　平成12年 3月14日
【手数料の表示】
【予納台帳番号】　014650
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9710074

【包括委任状番号】　0007553

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ送出装置、データ復号装置、データ送出方法、データ復号方法、伝送システム

【特許請求の範囲】

【請求項１】　デジタルデータをパケット化して送出するデータ送出装置において、

送出するパケットデータの一部に乱数データを挿入する挿入手段と、

上記挿入手段により乱数データが挿入されたパケットデータに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたパケットデータを送出する送出手段と、

を備えたことを特徴とするデータ送出装置。

【請求項２】　上記送出手段は、有線又は無線で接続された他の機器に対して上記パケットデータを送出することを特徴とする請求項１に記載のデータ送出装置。

【請求項３】　上記送出手段は、上記パケットデータを記録媒体に記録するデータとして送出することを特徴とする請求項１に記載のデータ送出装置。

【請求項４】　上記挿入手段は、パケットデータ内に存在する無効データ部分に、上記乱数データを挿入することを特徴とする請求項１に記載のデータ送出装置。

【請求項５】　上記暗号化手段は、上記パケットデータを１又は複数の所定の暗号化単位毎に暗号化処理を行うとともに、

上記挿入手段は、上記暗号化単位で乱数データを挿入することを特徴とする請求項１に記載のデータ送出装置。

【請求項６】　送出されてきたパケット化されたデジタルデータを入力する入力手段と、

上記入力手段により入力されたパケットデータに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたパケットデータから乱数データが挿入されたデータ

部分を除去する除去手段と、

を備えたことを特徴とするデータ復号装置。

【請求項７】　上記入力手段は、有線又は無線で接続された他の機器から送出されてきたパケットデータを入力することを特徴とする請求項６に記載のデータ復号装置。

【請求項８】　上記入力手段は、記録媒体から読み出されて送出されてきたパケットデータを入力することを特徴とする請求項６に記載のデータ復号装置。

【請求項９】　上記除去手段は、パケットデータ内に存在する無効データ部分を除去することで、乱数データが挿入されたデータ部分の除去を行うことを特徴とする請求項６に記載のデータ復号装置。

【請求項１０】　上記復号手段は、上記入力手段により入力されたパケットデータに対して、所定の暗号化単位で復号処理を行うとともに、

上記除去手段は、上記暗号化単位のデータから乱数データが挿入されたデータ部分を除去することを特徴とする請求項６に記載のデータ復号装置。

【請求項１１】　パケット化されたデジタルデータに対して、パケットデータの一部に乱数データを挿入し、

乱数データが挿入されたパケットデータに対して暗号化処理を行ない、

暗号化されたパケットデータを送出することを特徴とするデータ送出方法。

【請求項１２】　上記暗号化処理は、上記パケットデータを１又は複数の所定の暗号化単位で行われるとともに、

上記乱数データは、上記暗号化単位で挿入されることを特徴とする請求項１１に記載のデータ送出方法。

【請求項１３】　送出されてきたパケット化されたデジタルデータを入力し、

入力されたパケットデータに対して暗号化を解読する復号処理を行ない、

復号されたパケットデータから乱数データが挿入されたデータ部分を除去することを特徴とするデータ復号方法。

【請求項１４】　上記復号処理は、入力されたパケットデータに対して所定の暗号化単位で行なわれるとともに、

上記暗号化単位で復号されたデータから乱数データが挿入されたデータ部分が除去されることを特徴とする請求項１３に記載のデータ復号方法。

【請求項１５】　デジタルデータをパケット化して送出するデータ送出装置と、送出されてきたパケット化されたデジタルデータを復号する復号装置から成る伝送システムにおいて、

上記データ送出装置は、

送出するパケットデータの一部に乱数データを挿入する挿入手段と、

上記挿入手段により乱数データが挿入されたパケットデータに対して暗号化処理を行う暗号化手段と、

上記暗号化手段により暗号化されたパケットデータを送出する送出手段と、

を備え、

上記データ復号装置は、

送出されてきたパケット化されたデジタルデータを入力する入力手段と、

上記入力手段により入力されたパケットデータに対して暗号化を解読する復号処理を行う復号手段と、

上記復号手段で復号されたパケットデータから乱数データが挿入されたデータ部分を除去する除去手段と、

を備えたことを特徴とする伝送システム。

【請求項１６】　上記暗号化手段は、上記パケットデータを１又は複数の所定の暗号化単位毎に暗号化処理を行ない、

上記挿入手段は、上記暗号化単位で乱数データを挿入し、

上記復号手段は、上記入力手段により入力されたパケットデータに対して、上記暗号化単位で復号処理を行ない、

上記除去手段は、上記暗号化単位のデータから乱数データが挿入されたデータ部分を除去することを特徴とする請求項１５に記載の伝送システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は暗号化されたパケットデータの伝送を行う伝送システム、及びパケッ

トデータの伝送にかかるデータ送出装置、データ復号装置、データ送出方法、データ復号方法に関するものである。

【０００２】

【従来の技術】

例えば著作権保護が必要なデータ、秘密性の高いデータ、プライバシーにかかる私的データなど、外部に漏洩することが好ましくないデータの伝送に際しては、暗号化処理が行われることが多い。

例えば図１１に或る送信装置１０１から受信装置１０２に対してデータを暗号化して伝送するモデルを示す。

【０００３】

いま、伝送しようとするデータＤＴが送信装置１０１に入力されたとすると、送信装置１０１は、まず暗号化部１１１で暗号化処理を施し、暗号化されたデータＤＴｓを生成する。

そしてそのデータＤＴｓは送信部１１２から送信出力される。

送信出力されたデータＤＴｓは例えばＩＥＥＥ１３９４バスなどの伝送路１０３により、受信装置１０２に送られることになる。

受信装置１０２では、伝送路１０３から送信されてきたデータＤＴｓを受信部１２１で受信し、復号部１２２で暗号解読処理を行うことで、元のデータＤＴを得ることができる。

【０００４】

【発明が解決しようとする課題】

このように伝送路１０３においては暗号化されたデータＤＴｓが送信されることで、仮に伝送路１０３においてデータＤＴｓが取り出されたとしても、データＤＴの内容は秘密性が保たれるものとなる。

しかしながら、例えば著作権保護を目的として音楽データ等を図１１のようなシステムで伝送する場合、暗号を解読され、結果として違法なコピーが行われるおそれがある。

【０００５】

例えば伝送しようとするデータＤＴがＰＣＭオーディオデータであったとする

。

ＰＣＭオーディオデータの場合、無音部分、例えば曲と曲の間の期間に相当する部分や、再生装置等でアクセスが行われて、データとしてミュートパターンが配されている部分などでは、データストリーム上でゼロデータが並んでいるものとなっている。又は例えばΔΣ変調された１ビットオーディオデータの場合、無音部分は「９６ｈ」（＝１００１０１１０）などの固定パターンとなっている。

ここで、破線で示すように、何らかの手段で伝送路１０３から暗号化されたデータＤＴｓが取り出されたとする。

通常は、データＤＴｓを解析しても、元のデータＤＴ自体がわからないため、暗号の解読は困難である。

ところが、データＤＴｓにおいて、データＤＴの無音部分に相当する部分を抽出されると、元のデータがゼロデータ等の固定パターンであること、つまり元のデータの内容が明白となっていることから、比較的容易に暗号が解読され、データＤＴの内容や暗号化アルゴリズムが知られてしまう危険性がある。

もちろん暗号化アルゴリズムが解読されれば、悪意のユーザーによればその後データＤＴの違法な取り込みが容易に可能となってしまう。つまり著作権侵害となるような行為を実行可能としてしまう。

【０００６】

従って、音楽データ等の著作権保護が必要なデータについて、機器間の伝送、記録媒体への記録のための伝送、或いは公衆回線等を用いた音楽配信システムにおける伝送などの広範囲の分野で、上記の危険性が内包されており、このため違法な暗号解読を防止できるような技術が求められている。

【０００７】

【課題を解決するための手段】

本発明はこのような状況に鑑みて、伝送されるデータについて、容易に暗号解読ができないようにする技術を提供するものである。

【０００８】

このため本発明では、デジタルデータをパケット化して送出するデータ送出装置として、送出するパケットデータの一部に乱数データを挿入する挿入手段と、

上記挿入手段により乱数データが挿入されたパケットデータに対して暗号化処理を行う暗号化手段と、上記暗号化手段により暗号化されたパケットデータを送出する送出手段と、を備えるようにする。

例えば上記挿入手段は、パケットデータ内に存在する無効データ部分に、上記乱数データを挿入する。

また、上記暗号化手段は、上記パケットデータを１又は複数の所定の暗号化単位に分けて、該暗号化単位毎に暗号化処理を行うとともに、上記挿入手段は、上記暗号化単位で乱数データを挿入する。

【０００９】

また本発明のデータ復号装置は、送出されてきたパケット化されたデジタルデータを入力する入力手段と、上記入力手段により入力されたパケットデータに対して暗号化を解読する復号処理を行う復号手段と、上記復号手段で復号されたパケットデータから乱数データが挿入されたデータ部分を除去する除去手段と、を備えるようにする。

例えば上記除去手段は、パケットデータ内に存在する無効データ部分を除去することで、乱数データが挿入されたデータ部分の除去を行う。

またデータ送出装置側でパケットデータに対する暗号化処理が所定の暗号化単位で行われている場合は、上記復号手段は、上記入力手段により入力されたパケットデータに対して、所定の暗号化単位で復号処理を行うとともに、上記除去手段は、上記暗号化単位のデータから乱数データが挿入されたデータ部分を除去する。

【００１０】

また、本発明の伝送システムは、上記構成のデータ送出装置と上記構成のデータ復号装置により構成されるものとする。

そしてデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置としたり、記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装置における再生データの復号装置などとして実現されるようにする。

【００１１】

また本発明のデータ送出方法は、パケット化されたデジタルデータに対して、パケットデータの一部に乱数データを挿入し、乱数データが挿入されたパケットデータに対して暗号化処理を行ない、暗号化されたパケットデータを送出するものとする。

暗号化処理をパケットデータ内の所定の暗号化単位で行う場合は、暗号化単位のデータについて乱数データを挿入する。

【００１２】

本発明のデータ復号方法は、送出されてきたパケット化されたデジタルデータを入力し、入力されたパケットデータに対して暗号化を解読する復号処理を行ない、復号されたパケットデータから乱数データが挿入されたデータ部分を除去するようにする。

暗号化処理がパケットデータ内の所定の暗号化単位で行なわれている場合は、暗号化単位で復号処理を行い、その復号された暗号化単位のデータについて乱数データ部分を除去する。

【００１３】

即ち本発明では、暗号化を行う前にパケットデータ内に乱数データを挿入する。これによって、例えば元のデータにおいてゼロデータ列などの内容が明確な部分が存在しても、その部分が不明確な状態となるようにした上で暗号化されることとなるため、暗号アルゴリズムの解読は非常に困難なものとなる。

また特にパケットデータに対して、所定の暗号化単位で暗号化する場合は、その暗号化単位となるデータについて乱数データを挿入することで、より暗号アルゴリズムの解読を困難とする。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態を次の順に説明する。

１．送信装置及び受信装置に本発明を採用する例

２．ＩＥＥＥ１３９４の伝送フォーマット

３．ＩＥＥＥ１３９４でオーディオパケットデータを伝送する場合の乱数データ

挿入例１

４．ＩＥＥＥ１３９４でオーディオパケットデータを伝送する場合の乱数データ挿入例２

５．記録装置及び再生装置に本発明を採用する例

【００１５】

１．送信装置及び受信装置に本発明を採用する例

本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、送信装置、受信装置に採用する実施の形態を説明する。

図１は、或る２つの機器が例えばＩＥＥＥ１３９４バスによる伝送路３により接続されている場合に、送信装置１を有する機器から受信装置２を有する機器にデータＤＴを伝送するモデルにおいて本発明の実施の形態を示したものである。

パケット構造については後述するが、データＤＴは、例えば１ビットデジタルオーディオデータを、所定の伝送プロトコルに合致するフォーマットに基づいてパケット化（ブロック化）したものであるとする。

【００１６】

１ビットデジタルオーディオデータとは、通常のＣＤ（Compact Disc）におけるオーディオデータよりも高品位なデータとして開発されたものであり、サンプリング周波数を例えばＣＤ方式における４４．１ＫＨｚの１６倍という非常に高いサンプリング周波数である２．８４２ＭＨｚとしてΔΣ変調された１ビットデータのことであり、周波数帯域はＤＣ成分～１００ＫＨｚの広範囲とされ、ダイナミックレンジはオーディオ帯域全体で１２０（ｄＢ）を実現できるデータ形式である。

なお、本例ではこのような１ビットデジタルオーディオデータをパケット化して伝送する場合を例に挙げるが、もちろん伝送されるデータ自体の形式、種別はどのようなものでもよい。

【００１７】

図示するように送信装置１は、ランダムデータ付加部１１，暗号化部１２、送信部１３が設けられる。

ランダムデータ付加部１１は内部に乱数発生回路を備え、送信しようとするデータＤＴ（パケットデータ）の所要の部分に乱数発生回路で発生させた乱数データを付加する動作を行う。

暗号化部１２は、ランダムデータ付加部１１の出力に対して所定の暗号アルゴリズムでの暗号化処理を施す。

送信部１３は暗号化部１２の出力をＩＥＥＥ１３９４バスによる伝送路３に送出する動作を行う。

【００１８】

受信装置２は、受信部２１，復号部２２、ランダムデータ除去部２３を備える。

受信部２１は、伝送路３から供給されるデータを受信して取り込む動作を行う。

復号部２２は、上記暗号化部１２での暗号化アルゴリズムに対応して暗号解読処理を行う部位である。

ランダムデータ除去部２３は、上記ランダムデータ付加部１１で付加された乱数データ部分を除去する部位である。

【００１９】

このような送信装置１、受信装置２においてデータＤＴの伝送は次のように行われる。

パケットデータとして伝送しようとするデータＤＴが送信装置１に入力されたとすると、送信装置１は、まずランダムデータ付加部１１で、パケット内の所定の部位に乱数データを挿入する。具体例は後述するが、パケットデータ内の無効データ部分に乱数データを挿入することになる。

ランダムデータ付加部１１で乱数データが挿入されたデータＤＴａｄは、続いて暗号化部１２に供給され、暗号化処理が施される。

暗号化されたデータＤＴｓは、送信部１３に供給され、送信部１３から伝送路３に対して送出されることになる。

【００２０】

このように送信されたデータＤＴｓを受信する受信装置２では、まず伝送路３から供給されてきたデータＤＴｓを受信部２１で受信し、復号部２２に供給する。復号部ではデータＤＴｓに対する暗号解読処理を行うことで、暗号化前のデータ、即ち乱数データが付加されている状態のデータＤＴａｄが出力される。

このデータＤＴａｄはランダムデータ除去部２３に供給され、ランダムデータ部分が除去されることで、当初の送信データ、即ちデータＤＴが得られることとなる。

【００２１】

ここで破線で示すように、何らかの手段で伝送路３から暗号化されたデータＤＴｓが取り出された場合を考える。

上述したようにデータＤＴｓにおいて元の内容が明白な部分（無音部分）が抽出されると暗号化アルゴリズムが解読されるおそれがある。

しかしながら本例の場合、データＤＴｓは、乱数データが付加された上で暗号化されたものである。つまりゼロデータ等の固定パターンが連続する部分がなくされた状態で暗号化されている。従ってデータＤＴｓから、無音部分に相当するデータ部分を抽出することは困難となり、この点で暗号解読は困難となる。

また、仮にデータＤＴｓにおいて、元の１ビットデジタルオーディオデータとしての無音部分、即ちゼロデータが連続している部分に相当する部分が抽出され、データＤＴ（つまりゼロデータ）とＤＴｓが比較解析されたとする。

ところがこの場合でも、データＤＴｓは、乱数データを含めた上で暗号化されているため、データＤＴｓの解析処理において、データＤＴｓ上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することはほぼ不可能である。

【００２２】

以上のことから、本例によれば伝送路３で伝送されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの伝送などに非常に好適なものとなる。

また送信装置１側では従前の構成にランダムデータ付加部１１を設けるだけで

よく、受信装置２側では、ランダムデータ除去部２３を設けて、暗号化を解読したうえで乱数データが挿入されたデータ部分を除去するのみでデータを復号できる。従って送信装置１，受信装置２としての構成がさほど複雑化することもなく、各種の機器への導入は容易なものとなる。

【００２３】

２．ＩＥＥＥ１３９４の伝送フォーマット

ここでＩＥＥＥ１３９４による伝送フォーマットについて説明する。

ＩＥＥＥ１３９４方式でのデータ伝送では、例えば図２（ａ）に示すように、所定の通信サイクル（例えば１２５μｓｅｃ）毎に時分割多重によって行われる。そして、この信号の伝送は、サイクルマスタと呼ばれる機器（ＩＥＥＥ１３９４バス上の任意の１台の機器）が通信サイクルの開始時であることを示すサイクルスタートパケットＣＳＰをバス上へ送出することにより開始される。なお、サイクルマスタは、バスを構成するケーブルに各機器を接続したとき等に、ＩＥＥＥ１３９４で規定する手順により自動的に決定される。

【００２４】

１通信サイクル中における通信の形態は、ビデオデータやオーディオデータなどのリアルタイム性を必要とするデータを伝送するアイソクロナス伝送（Ｉｓｏ）と、制御コマンドや補助的なデータなどを確実に伝送するアシンクロナス伝送（Ａｓｙ）の２種類の伝送が行われる。

各通信サイクル中では、アイソクロナス伝送用のアイソクロナスパケットＩｓｏが、アシンクロナス伝送用のアシンクロナスパケットＡｓｙより先に伝送される。

アイソクロナスパケットＩｓｏの通信が終了した後、次のサイクルスタートパケットＣＳＰまでの期間が、アシンクロナスパケットＡｓｙの伝送に使用される。従って、アシンクロナスパケットＡｓｙが伝送できる期間は、そのときのアイソクロナスパケットＩｓｏの伝送チャンネル数により変化する。また、アイソク

ロナスパケットＩｓｏは、１通信サイクル毎に予約した帯域（チャンネル数）が確保される伝送方式であるが、受信側からの確認は行わない。

アシンクロナスパケットＡｓｙで伝送する場合には、受信側からアクノリッジメント（Ａｃｋ）のデータを返送させて、伝送状態を確認しながら確実に伝送させる。

【００２５】

図２（ｂ）に、ＣＩＰ(Common Isochronos Packet)の構造を示す。つまり、図２（ａ）に示したアイソクロナスパケットＩｓｏのデータ構造である。

例えば、上述した１ビットデジタルオーディオデータは、ＩＥＥＥ１３９４通信においては、アイソクロナス通信によりデータの送受信が行われる。つまり、リアルタイム性が維持されるだけのデータ量をこのアイソクロナスパケットに格納して、１アイソクロナスサイクル毎に順次送信するものである。

【００２６】

アイソクロナスパケットは、図２（ｂ）のように、１３９４パケットヘッダ、ヘッダＣＲＣ、ＣＩＰヘッダ、データ部、データＣＲＣから成る。

このＣＩＰ構造として、例えば２チャンネルの１ビットデジタルオーディオデータの伝送に用いる場合における具体例を図３に示している。

【００２７】

図３では、横方向に３２ビット（４バイト）を示しているが、その１行分のデータ、つまり３２ビットが１カドレット（ｑｕａｄｌｅｔ）と呼ばれる。

ＣＩＰの先頭３２ビット（１カドレット）は、１３９４パケットヘッダとされている。

１３９４パケットヘッダにおいては、１６ビットのデータレングス（ｄａｔａ＿Ｌｅｎｇｔｈ）、２ビットのタグ（ｔａｇ）、６ビットのチャンネル（ｃｈａｎｎｅｌ）、４ビットのタイムコード（ｔ　ｃｏｄｅ）、４ビットのシンク（ｓｙ）が配される。

そして、１３９４パケットヘッダに続く１カドレットの領域はヘッダＣＲＣが格納される。

【００２８】

ヘッダＣＲＣに続く２カドレットの領域がＣＩＰヘッダとなる。

ＣＩＰヘッダの上位カドレットの先頭２バイトには、それぞれ‘０’‘０’が格納され、続く６ビットの領域はＳＩＤ（送信ノード番号）を示す。ＳＩＤに続く８ビットの領域はＤＢＳ（データブロックサイズ）であり、データブロックのサイズ（パケット化の単位データ量）が示される。続いては、ＦＮ（２ビット）、ＱＰＣ（３ビット）の領域が設定されており、ＦＮにはパケット化する際に分割した数が示され、ＱＰＣには分割するために追加したカドレット数が示される。

ＳＰ（１ビット）にはソースパケットのヘッダのフラグが示され、ＤＢＣにはパケットの欠落を検出するカウンタの値が格納される。

なお、図中「ｒｓｖ」はリザーブ、つまり未定義の領域を示している。

【００２９】

ＣＩＰヘッダの下位カドレットの先頭２バイトにはそれぞれ‘１’‘０’が格納される。そして、これに続いてＦＭＴ（６ビット）、ＦＤＦ（８ビット）、ＳＹＴ（１６ビット）の領域が設けられる。

ＦＭＴには信号フォーマット（伝送フォーマット）が示され、ここに示される値によって、当該ＣＩＰに格納されるデータ種類（データフォーマット）が識別可能となる。具体的には、ＭＰＥＧストリームデータ、Ａｕｄｉｏストリームデータ、デジタルビデオカメラ（ＤＶ）ストリームデータ等の識別が可能になる。

ＦＤＦは、フォーマット依存フィールドであり、上記ＦＭＴにより分類されたデータフォーマットについて更に細分化した分類を示す領域とされる。オーディオに関するデータであれば、例えばリニアオーディオデータであるのか、ＭＩＤＩデータであるのかといった識別が可能になる。

例えば１ビットデジタルオーディオデータであれば、先ずＦＭＴによりＡｕｄｉｏストリームデータの範疇にあるデータであることが示され、ＦＤＦに規定に従った特定の値が格納されることで、そのＡｕｄｉｏストリームデータは１ビットデジタルオーディオデータであることが示される。

ＳＹＴは、フレーム同期用のタイムスタンプが示される。

【００３０】

このようなＣＩＰヘッダに続けては、ＦＭＴ，ＦＤＦによって示されるデータが、データ部としてのｎ個のデータブロック（ブロック＃０～＃ｎ）のシーケンスによって格納される。ＦＭＴ，ＦＤＦにより１ビットデジタルオーディオデータであることが示される場合には、このデータブロックとしての領域に１ビットデジタルオーディオデータが格納される。

そして、データブロックに続いて最後にデータＣＲＣが配置される。

【００３１】

この図３では、データ部に２チャンネルの１ビットデジタルオーディオデータが配されている例を示している。これは、ＩＥＥＥ１３９４バスによるデータ伝送について適用できるＡＭ８２４と呼ばれる伝送プロトコルに基づいた例であり、その場合において１ビットデジタルオーディオデータとして２チャンネルのオーディオデータを伝送する場合のパケット構造例である。

【００３２】

上述のように３２ビット（４バイト）を１カドレット（Quadlet）と呼ぶとすると、２チャンネルデータの場合、４カドレット（ｑ１～ｑ４）で１つのブロックが形成され、このブロックが連続するものとなる。

【００３３】

各カドレットにおける先頭のバイト（バイト０）は、ラベルとされている。ラベルとは、そのカドレットに配されるデータの識別情報となる。

ラベルとしての値及び意味を図４に示す。

図示するようにラベル値に対して各種の意味が定義されており、例えばラベル値４０ｈ～４Ｆｈは、ＤＶＤ（Digital Versatile Disc）システムで採用されているマルチビットリニアオーディオデータに対応するものとされる。なお、「ｈ」を付した数値は１６進表記のものである。

またラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値、ラベル値５８ｈ～５Ｆｈは、エンコードされた１ビットデジタルオーディオデータに対応する値、ラベル値８０ｈ～８３ｈはＭＩＤＩデータに対応する値とされる。

さらにＣ０ｈ～ＥＦｈはアンシラリデータ（Ancillary Data；補助データ）を

意味するなど、ラベル値は識別情報として機能するために各種定義されている。

【００３４】

各ラベル値についての詳細な定義の説明は本発明と直接関係がないため説明を省略するが、図３に示した値についてのみ述べると次のようになる。

【００３５】

図３においてブロック＃０の第１カドレットｑ１をみると、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「００ｈ」とされている。

このときバイト２，バイト３が実際の補助データ内容となるが、ここではバリディティフラグ（Validity Flag）Ｖ、コピーコントロール情報（Track Attribute）、チャネル数（Ch Bit Num）、スピーカ配置情報（Loudspeaker Config）が記述される。

【００３６】

第２カドレットｑ２ではラベル値は「５０ｈ」とされる。ラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値であるが、「５０ｈ」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第３カドレットｑ３ではラベル値は「５１ｈ」とされる。「５１ｈ」は、マルチチャンネルのデータを配したブロックの２番目以降のデータであることを示す。

従って、第２、第３カドレット（ｑ２、ｑ３）では、チャンネル１、チャンネル２の２チャンネルの１ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト１～バイト３の３バイトで記述される。

【００３７】

第４カドレットｑ４では、ラベル値は「ＣＦｈ」とされている。これはアンシラリデータの範疇であるが、「ＣＦｈ」は特に無効データ（NO DATA）を示す値として定義されている。またバイト１はサブラベルとして無効データの内容を示

す値とされており、この例では「ＣＦｈ」とされている。

そしてこのときバイト２，バイト３が無効データにより充填される。

【００３８】

ブロック＃１の第１カドレットｑ１では、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「０１ｈ」とされている。

このときはバイト２，バイト３の補助データ内容は、サプリメンタリデータとされる。

第２～第４カドレットはブロック＃０と同様である。

【００３９】

このように各ブロックが構成されて、アイソクロナスパケットＩｓｏにおけるデータ部が形成される。

【００４０】

３．ＩＥＥＥ１３９４でオーディオパケットデータを伝送する場合の乱数データ挿入例１

以上のようなＩＥＥＥ１３９４による伝送フォーマットを用いて、図１で説明したようにデータを伝送する場合の具体例を以下、説明していく。即ちＩＥＥＥ１３９４の伝送路３でオーディオパケットデータを伝送する場合の乱数データ挿入方式の例である。

【００４１】

図５は送信しようとするデータＤＴとしてのデータパケット構造例を示している。これは、ＩＥＥＥ１３９４バスによるデータ伝送について適用できるＡＭ８２４の伝送プロトコルに基づき、１ビットデジタルオーディオデータとして６チャンネルのオーディオデータを伝送する場合のパケット構造例を示している。

なお、図５にフレームとして示すブロック＃０～＃１５６７の部分は、図２，

図３で説明したアイソクロナスパケットＩｓｏ内のデータ部に相当する部分である。

【００４２】

６チャンネルデータの場合、８カドレット（ｑ１～ｑ８）で１つのブロックが形成され、このブロックが連続するものとなる。

１５６８ブロックの範囲が１フレームと呼ばれる単位となる。

そして１ビットデジタルオーディオデータとしての伝送データストリームは、このようなフレームが連続されて形成される。

【００４３】

この場合、ブロック＃０の第１カドレットｑ１をみると、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「００ｈ」とされている。図３で説明したように、バイト２，バイト３の補助データ内容としては、コピーコントロール情報、チャネル数、スピーカ配置情報等が記述される。

【００４４】

第２カドレットｑ２ではラベル値は「５０ｈ」とされる。ラベル値５０ｈ～５７ｈは、１ビットデジタルオーディオデータに対応する値であるが、「５０ｈ」は、マルチチャンネルのデータを配したブロックの最初のデータであることを示す。

また第３～第７カドレット（ｑ３～ｑ７）ではラベル値は「５１ｈ」とされる。「５１ｈ」は、マルチチャンネルのデータを配したブロックの２番目以降のデータであることを示す。

従って、第２～第７カドレット（ｑ１～ｑ７）では、チャンネル１～チャンネル６の６チャンネルの１ビットデジタルオーディオデータが配されていることが示されるものとなる。各チャンネルのデータはバイト１～バイト３の３バイトで記述される。

【００４５】

第８カドレットｑ８では、ラベル値は「ＣＦｈ」とされている。これはアンシ

ラリデータの範疇であるが、「ＣＦｈ」は特に無効データ（NO DATA）を示す値として定義されている。

またこの場合は、バイト１は無効データの内容を示す値とされており、この例のような「５０ｈ」は１ビットデジタルオーディオデータとしての無効データを示すものとなる。

そしてこのときバイト２，バイト３が無効データにより充填される。

【００４６】

ブロック＃１の第１カドレットｑ１では、ラベル値は「Ｄ１ｈ」とされている。従って第１カドレットｑ１はアンシラリデータが記述されるものと提示されていることになり、さらにこの場合バイト１はサブラベルとされて「０１ｈ」とされている。

このときはバイト２，バイト３の補助データ内容は、サプリメンタリデータとされる。

第２～第８カドレットはブロック＃０と同様である。

【００４７】

ブロック＃１５６７の第１カドレットｑ１では、ラベル値は「ＣＦｈ」とされている。つまりバイト２，バイト３は無効データである。ただし、バイト１は「Ｄ１ｈ」とされていることで、アンシラリデータとしての無効データであることが示されている。

第２～第８カドレットはブロック＃０と同様である。

【００４８】

例えばこのようなパケットデータストリームを伝送する場合を例に挙げると、上述した送信装置１のランダムデータ付加部１１では、無効データの部分に乱数データを挿入すればよい。

即ち各パケットにおいて斜線部を付した無効データ部分に乱数データを挿入する。具体的にはランダムデータ付加部１１では１パケットあたりに２バイトの乱数データを生成し、無効データのカドレット、つまりラベル値＝「ＣＦｈ」のカドレットのバイト２，３の２バイトに挿入するものである。

このように乱数データを挿入することにより、パケット内のオーディオデータ

が仮にオールゼロ、あるいは「９６ｈ」などの固定パターンであったとしても、オールゼロあるいは「９６ｈ」等とは見えないものとなり、上述の通り、暗号解読を防止できるものとなる。

【００４９】

また、このように無効データ部分に乱数データを挿入することは、受信装置２側での処理が非常に簡単となることを意味する。

即ち受信装置１０２の復号部２２で暗号解読処理が施されると、図５の状態のパケットデータストリームがランダムデータ除去部２３に供給されることになるが、ランダムデータ除去部２３では、ラベル値＝「ＣＦｈ」のカドレットを捨てればよいのみとなる。

ラベル値＝「ＣＦｈ」のカドレットは無効データとして本来捨てられるものであるため、その意味でいえば、ランダムデータ除去部２３は何ら特別な処理を必要としないものともなる。

【００５０】

４．ＩＥＥＥ１３９４でオーディオパケットデータを伝送する場合の乱数データ挿入例２

上記図５の例では、各ブロック＃０～＃１５６７において、無効データが配されることになるカドレットｑ８に乱数データを挿入する例を述べた。つまり１ブロックのうちの１つのカドレットのみに乱数データを挿入した。

ところが、例えば図１の送信装置１の暗号化部１２において、例えば１ブロックよりも少ないデータ単位で暗号化を行うように伝送フォーマット上で規定されている場合は、暗号解読が可能となってしまう場合がある。

例えば暗号化部１２で暗号化を行うデータ単位（暗号化単位）が８バイト（２カドレット）であるとされている場合、乱数データが挿入されていない部分が解析されることが起こり得る。

【００５１】

例えば暗号化単位が８バイトであるとして図５のブロック＃０について考えてみる。このとき、ブロック＃０のオーディオデータが仮にオールゼロ、あるいは「９６ｈ」などの固定パターンであったとする。

暗号化処理は、カドレットｑ１，ｑ２、カドレットｑ３，ｑ４、カドレットｑ５，ｑ６、カドレットｑ７，ｑ８の、それぞれの暗号化単位で行われるが、このときカドレットｑ３，ｑ４、及びカドレットｑ５，ｑ６の２つの暗号化単位の部分は、乱数データが付加された上での暗号化処理とはならない。

【００５２】

従って、カドレットｑ３，ｑ４、もしくはカドレットｑ５，ｑ６の部分が抽出されると、実データはオールゼロ、あるいは「９６ｈ」などの固定パターンであることから暗号化アルゴリズムが不正に解読されるというおそれがある。

なお、カドレットｑ１，ｑ２の暗号化単位では、既に暗号化されたアンシラリデータが挿入されていることで、データがオールゼロ、あるいは「９６ｈ」などの固定パターンとならないため、暗号解読は困難である。またカドレットｑ７，ｑ８の暗号化単位では、乱数データにより暗号解読が困難となることはいうまでもない。

【００５３】

そこで、暗号化単位がブロック単位でない場合、つまり１つのブロックよりも小さい単位で暗号化を行う場合は、以下のように乱数データを挿入することが好適となる。

【００５４】

図６にＬ、Ｒの２チャンネルの１ビットデジタルオーディオデータを伝送する場合の例を示す。

なお、図６（ａ）（ｂ）（ｃ）は、図３、図５で説明した構造のブロックとしてのブロック＃０～＃１５６７を、楽曲としてのトラック、及びトラックを構成するフレームとともに示しているものである。

公知のように１つのフレームは７５Ｈｚ周期、即ち１３．３ｍｓｅｃ分のオーディオデータに相当する単位である。

上述したように１フレームは１５６８ブロックで構成されるが、２チャンネル

データの場合、各ブロック＃０～＃１５６７は、図６（ｄ）のようになる。

暗号化単位ＥＵは８バイトとされ、従って第１，第２カドレットの暗号化単位ＥＵ１で暗号化処理が行われるとともに、第３，第４カドレットの暗号化単位ＥＵ２で暗号化処理が行われる。つまり１ブロックは２つの暗号化単位ＥＵで構成される。

【００５５】

この場合、図１の送信装置１のランダムデータ付加部１１は、各暗号化単位ＥＵにおいて、少なくとも、データがオールゼロ又は固定パターンとなる可能性のある暗号化単位に乱数データを付加するようにする。

従って、まずブロック＃０では、暗号化単位ＥＵ２の無効データ部分とされる第４カドレットのバイト２，バイト３（＝斜線部）に乱数データを挿入する。ブロック＃１も同様である。

またブロック＃ｘ～＃１５６７においては、暗号化単位ＥＵ１内で第１カドレットが無効データ部分とされるとすると、その無効データが配されるバイト２，バイト３（＝斜線部）に乱数データを挿入する。また暗号化単位ＥＵ２の無効データ部分とされる第４カドレットのバイト２，バイト３（＝斜線部）にも乱数データを挿入する。

このように乱数データが挿入された後に、暗号化部１２で暗号化が施されて伝送路３に送出される。

【００５６】

ブロック＃０、＃１・・・＃（ｘ－１）では、第１カドレットにアンシラリデータが挿入されているとすると、暗号化単位ＥＵ１では、データがオールゼロ又は固定データのみとはならないため、この部分で暗号化アルゴリズムが解読できることはない。そして暗号化単位ＥＵ２でも乱数データが挿入されることで、例えオーディオデータが固定パターンであっても暗号解読は困難となる。つまりどちらの暗号化単位が抽出されても、暗号化アルゴリズムが解読されるおそれはない。

またブロック＃ｘ～＃１５６７においては暗号化単位ＥＵ１，ＥＵ２ともに乱数データが挿入されているため、どちらの暗号化単位が抽出されても暗号化アル

ゴリズムが解読されるおそれはない。

【００５７】

また、このような乱数データ挿入例の場合も、無効データ部分に乱数データを挿入するため、受信装置２側での処理が非常に簡単となる。

即ち受信装置１０２の復号部２２で暗号解読処理が施されると、図６（ｄ）の状態のパケットデータストリームがランダムデータ除去部２３に供給されることになるが、ランダムデータ除去部２３では、ラベル値＝「ＣＦｈ」のカドレットを捨てればよいのみとなる。

【００５８】

同様に、暗号化単位ＥＵで乱数データを挿入する例として、５チャンネルオーディオデータの場合を図７に、また６チャンネルオーディオデータの場合を図８に、それぞれ示す。

【００５９】

図７（ａ）は、５チャンネルの１ビットデジタルオーディオデータを伝送する場合のブロック＃０～＃１５６７を示している。

５チャンネルオーディオデータの場合、基本的には１つのブロックは図７（ｂ）のよう６カドレットで形成されることになるが、本例では暗号化単位ＥＵについて乱数データを挿入するようにするために、無効データが配されるカドレット（ラベル＝「ＣＦｈ」となるカドレット）を追加的に付加し、図７（ａ）のように１ブロックが１０カドレットで形成されるようにしている。

これにより１ブロックは５つの暗号化単位ＥＵ１～ＥＵ５で構成されるとともに、暗号化単位ＥＵ２～ＥＵ５には、それぞれ無効データ部分が設けられることになる。

【００６０】

この場合も、図１の送信装置１のランダムデータ付加部１１は、各暗号化単位ＥＵにおいて、少なくとも、データがオールゼロ又は固定パターンとなる可能性のある暗号化単位ＥＵに乱数データを付加するようにする。

従って、まずブロック＃０では、暗号化単位ＥＵ２～ＥＵ５について、それぞれ無効データ部分（斜線部）に乱数データを挿入する。ブロック＃１も同様であ

る。

またブロック＃ｘ～＃１５６７においては、暗号化単位ＥＵ１内で第１カドレットが無効データ部分とされるとすると、その無効データが配されるバイト２，バイト３（＝斜線部）に乱数データを挿入する。また暗号化単位ＥＵ２～ＥＵ５についても、それぞれ無効データ部分（斜線部）に乱数データを挿入する。

このように乱数データが挿入された後に、暗号化部１２で暗号化が施されて伝送路３に送出される。

【００６１】

このような処理によって上記の２チャンネルの場合と同様に、どの暗号化単位が抽出されても、暗号化アルゴリズムが解読されるおそれはない。

また、受信装置２側での処理が簡単であることも同様である。

【００６２】

図８（ａ）は、６チャンネルの１ビットデジタルオーディオデータを伝送する場合のブロック＃０～＃１５６７を示している。

６チャンネルオーディオデータの場合、基本的には１つのブロックは図８（ｂ）のよう８カドレットで形成されることになるが、本例ではこの場合も、暗号化単位ＥＵについて乱数データを挿入するようにするために、無効データが配されるカドレット（ラベル＝「ＣＦｈ」となるカドレット）を追加的に付加し、図８（ａ）のように１ブロックが１２カドレットで形成されるようにしている。

これにより１ブロックは６つの暗号化単位ＥＵ１～ＥＵ６で構成されるとともに、暗号化単位ＥＵ２～ＥＵ６には、それぞれ無効データ部分が設けられることになる。

【００６３】

この場合も、図１の送信装置１のランダムデータ付加部１１は、各暗号化単位ＥＵにおいて、少なくとも、データがオールゼロ又は固定パターンとなる可能性のある暗号化単位ＥＵに乱数データを付加する。

従って、まずブロック＃０では、暗号化単位ＥＵ２～ＥＵ６について、それぞれ無効データ部分（斜線部）に乱数データを挿入する。ブロック＃１も同様である。

またブロック＃ｘ～＃１５６７においては、暗号化単位ＥＵ１内で第１カドレットが無効データ部分とされるとすると、その無効データが配されるバイト２，バイト３（＝斜線部）に乱数データを挿入する。また暗号化単位ＥＵ２～ＥＵ５についても、それぞれ無効データ部分（斜線部）に乱数データを挿入する。

このように乱数データが挿入された後に、暗号化部１２で暗号化が施されて伝送路３に送出される。

【００６４】

このような処理によって上記の２チャンネルの場合と同様に、どの暗号化単位が抽出されても、暗号化アルゴリズムが解読されるおそれはない。

また、受信装置２側での処理が簡単であることも同様である。

【００６５】

５．記録装置及び再生装置に本発明を採用する例

続いて、本発明のデータ送出装置（データ送出方法）、データ復号装置（データ復号方法）を、記録装置、再生装置に採用する実施の形態を説明する。

記録装置は記録媒体に対するデータ送出装置となり、また再生装置は記録媒体から読み出されたデータのデータ復号装置となる。

【００６６】

図９は所定の記録媒体（メディア）６に対してデータＤＴを記録できる記録装置である。

図示するように記録装置４は、入力されてくるデータＤＴに対する記録処理系として、暗号化部４０，エンコード及び記録ドライブ部４４、記録ヘッド（又はインターフェース）４５が設けられる。

暗号化部４０は、ランダムデータ付加部４１，暗号化部４２、送出部４３を有する。

【００６７】

このような記録装置４では、入力されたデータＤＴについて、ランダムデータ

付加部４１は内部に乱数発生回路から発生させた乱数データを、データＤＴの所要の部分に付加する。

ランダムデータ付加部４１で乱数データが挿入されたデータＤＴａｄは、続いて暗号化部４２に供給され、暗号化処理が施される。

暗号化されたデータＤＴｓは、送出部４３に供給され、送出部４３からエンコード及び記録ドライブ部４４に送出される。

エンコード及び記録ドライブ部４４は、供給されたデータＤＴｓに対して、記録を行うメディア６の記録フォーマット、変調方式に応じてエラー訂正符号の付加や各種エンコード処理を行い、記録ドライブ信号を生成する。

その記録ドライブ信号は記録ヘッド４５に供給されて記録ヘッド４５によりメディア６へのデータ書込が行われる。

例えばメディア６が光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどであれば、記録ドライブ信号に応じて光学ヘッド又は磁気ヘッドが駆動されて記録が実行される。

また、メディア６がフラッシュメモリなどによるメモリカードのような形態であれば、インターフェース４５によりメディア６に対して書込アクセスが行われることになる。

【００６８】

図１０は所定の記録媒体（メディア）６からデータＤＴを再生できる再生装置である。

図示するように再生装置５は、メディア６からデータの読み出しを行う再生ヘッド（又はインターフェース）５４、デコード部５５、復号部５０が設けられる。

復号部５０は、取込部５１，復号部５２、ランダムデータ除去部５３を備える。

【００６９】

この再生装置５では、例えばメディア６としての光ディスク、光磁気ディスク、磁気ディスク、磁気テープなどから光学ヘッド又は磁気ヘッドとしての再生ヘッド５４によって読み出されたデータ、或いはメディア６としてのメモリカード

からインターフェース５４を介した読出アクセスにより読み出されたデータは、デコード部５５で、メディア６の記録フォーマットに応じたデコード処理やエラー訂正処理が行われる。そしてそのデコードされたデータは、即ち記録装置４で暗号化されたデータＤＴｓであり、データＤＴｓは取込部５１により復号部５０内に取り込まれ、復号部５２で暗号解読処理される。

復号部５２で、上記暗号化部４２での暗号化アルゴリズムに対応した暗号解読処理を行うことで、ランダムデータが付加された状態のデータＤＴａｄとされる。そして、そのデータＤＴａｄがランダムデータ除去部５３に供給されて、上記ランダムデータ付加部４１で付加された乱数データ部分が除去されることで、元のデータＤＴが再生されるものとなる。

【００７０】

記録装置４，再生装置５が以上のように構成されることで、メディア６に記録されるデータは、乱数データが付加された上で暗号化されたデータＤＴｓがエンコードされたものである。つまり例えば元のオーディオデータとしてゼロデータが連続する部分があったとしても、そのゼロデータ等の固定パターンが連続する部分がなくされた状態で暗号化されたデータがエンコードされている。

従ってメディア６に記録されたデータをデコードしても、無音部分に相当するデータ部分を抽出することは困難となり、この点で暗号解読は困難となる。

さらにゼロデータが連続している部分に相当する部分が抽出され、データＤＴ（つまりゼロデータ）とＤＴｓが比較解析されたとしても、データＤＴｓは、乱数データを含めた上で暗号化されているため、データＤＴｓの解析処理において、データＤＴｓ上では暗号化アルゴリズムによるデータ要素と乱数データによるデータ要素を区別することはできず、従って、暗号化アルゴリズムを解析することはほぼ不可能である。

もちろん乱数データが挿入されるのは、上記図５で説明したようにブロック内の１つのカドレットとしたり、或いは図６、図７、図８で説明したように暗号化単位内のカドレットとすればよい。

また無効データ部分に乱数データを挿入することで、再生装置５側でのランダムデータ除去処理は容易なものとなる。

【００７１】

つまりこのような記録装置、再生装置によれば、メディア６に記録されるデータについて暗号解読は非常に困難なものとなり、従って、著作権保護を要するデータの記録などに非常に好適なものとなる。また、上述した送信装置１，受信装置２の場合と同様に、記録装置４、再生装置５として構成がさほど複雑化することもなく、導入は容易である。

【００７２】

なお、図９，図１０として記録装置４、再生装置５を分けて示したが、これらの回路構成を１つの機器に設けて、記録再生装置とすることはもちろん可能である。

また、記録装置４（又は記録再生装置）としては、必ずしも暗号化部４０を設けなくてもよい。例えば伝送路３を介して或る送信装置から伝送されてきたデータを記録する記録装置を考えると、その送信装置側が図１に示した構成を備えていれば、記録装置に伝送されてくるデータは、既に乱数データが付加された上で暗号化されたデータＤＴｓとなっている。従ってその場合、記録装置は暗号化部４０は不要となる。そして再生装置は、図１０に示した復号部５０を備えることで、伝送され記録されたデータの再生を行うことができるようになる。

例えば音楽等の配信システムなどを想定すると、このような形態が好適なものとなる。

【００７３】

以上、実施の形態を説明してきたが、本発明はさらに多様な構成例が考えられ、また送信装置、受信装置、記録装置、再生装置などの形態で多種多様な機器に導入できるものである。

また、上記例では送信装置１と受信装置２は有線としてのＩＥＥＥ１３９４方式の伝送路３による伝送システムとしたが、他の伝送規格によるものでもよく、また衛星通信、無線電話通信、赤外線伝送などの無線伝送システムに本発明を適用できることはもちろんである。

また、伝送するデータは図５～図８に示したようなブロックデータに限定されるものではなく、あらゆるデータの伝送に本発明を適用できる。特に本発明でい

う「パケット」とは広い意味であり、一般に「ブロック」「フレーム」「セクター」「クラスタ」などと呼ばれる各種データ単位を含むものである。

【００７４】

【発明の効果】

以上の説明からわかるように、本発明によれば、伝送するデータについて、パケットデータ内に乱数データを挿入したうえで暗号化を行なって伝送するようにしている。このため、例えば元のデータにおいてゼロデータ列などの内容が明確な部分が存在しても、その部分が不明確な状態となるようにした上で暗号化されることとなるため、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読は非常に困難なものとなるという効果があり、従って著作権保護などに好適なものとなる。

また、このように乱数データが付加された上で暗号化されたデータを復号する場合は、暗号化を解読したうえで乱数データが挿入されたデータ部分を除去するのみでデータを復号できるため、復号のために複雑な処理は必要なく、簡易な構成で復号装置を実現でる。

換言すれば本発明では、データ送出装置、データ復号装置としては装置構成の複雑化を招かずに、暗号解読が非常に困難なデータ伝送を実現できるものとなる。

【００７５】

また本発明では、データ送出装置側では、パケットデータ内に存在する無効データ部分に乱数データを挿入することで、パケットとしての構造を保ったまま本発明の効果を実現でき、伝送方式やパケット仕様の変更やそれに伴う処理の変更なども不要であるため、従前の伝送システムなどに容易に導入できる。

またその場合、データ復号装置側では、パケットデータ内に存在する無効データ部分を除去するというのみで、乱数データが挿入されたデータ部分の除去を行うことができるため処理は非常に容易なものとなる。

【００７６】

またデータ送出装置とデータ復号装置は、それぞれ異なる機器間における送信装置、受信装置とすることで、機器間のデータ伝送において上記効果を実現でき

る。

さらにデータ送出装置とデータ復号装置は、それぞれ記録媒体に記録を行う記録装置における記録データの送出装置、記録媒体からデータの再生を行う再生装置における再生データの復号装置とすることで、記録媒体に記録されているデータ、又は記録再生の過程のデータにおいて上記効果を実現できる。

【００７７】

また特に、暗号化処理を行う暗号化単位で乱数データを挿入するようにすることで、暗号化処理がパケット（ブロック）よりも小さい暗号化単位で行われる場合でも、暗号解読を困難とすることができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態の送信装置及び受信装置のブロック図である。

【図２】

ＩＥＥＥ１３９４による伝送フォーマットの説明図である。

【図３】

ＩＥＥＥ１３９４のアイソクロナスパケットの説明図である。

【図４】

実施の形態のパケットデータのラベルの説明図である。

【図５】

実施の形態の乱数データ挿入例の説明図である。

【図６】

実施の形態の乱数データ挿入例の説明図である。

【図７】

実施の形態の乱数データ挿入例の説明図である。

【図８】

実施の形態の乱数データ挿入例の説明図である。

【図９】

実施の形態の記録装置のブロック図である。

【図１０】

実施の形態の再生装置のブロック図である。

【図１１】

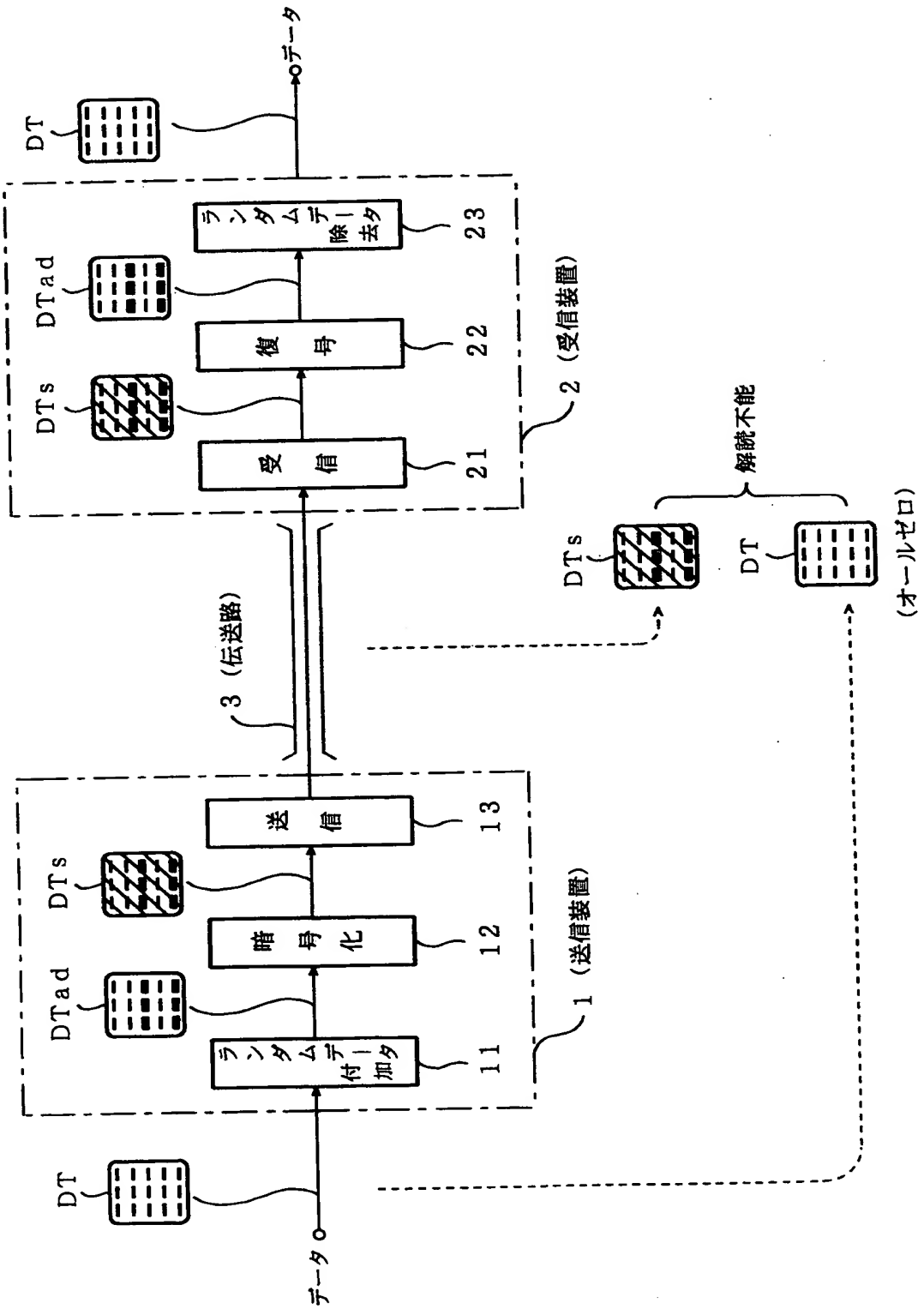
従来の伝送システムの説明図である。

【符号の説明】

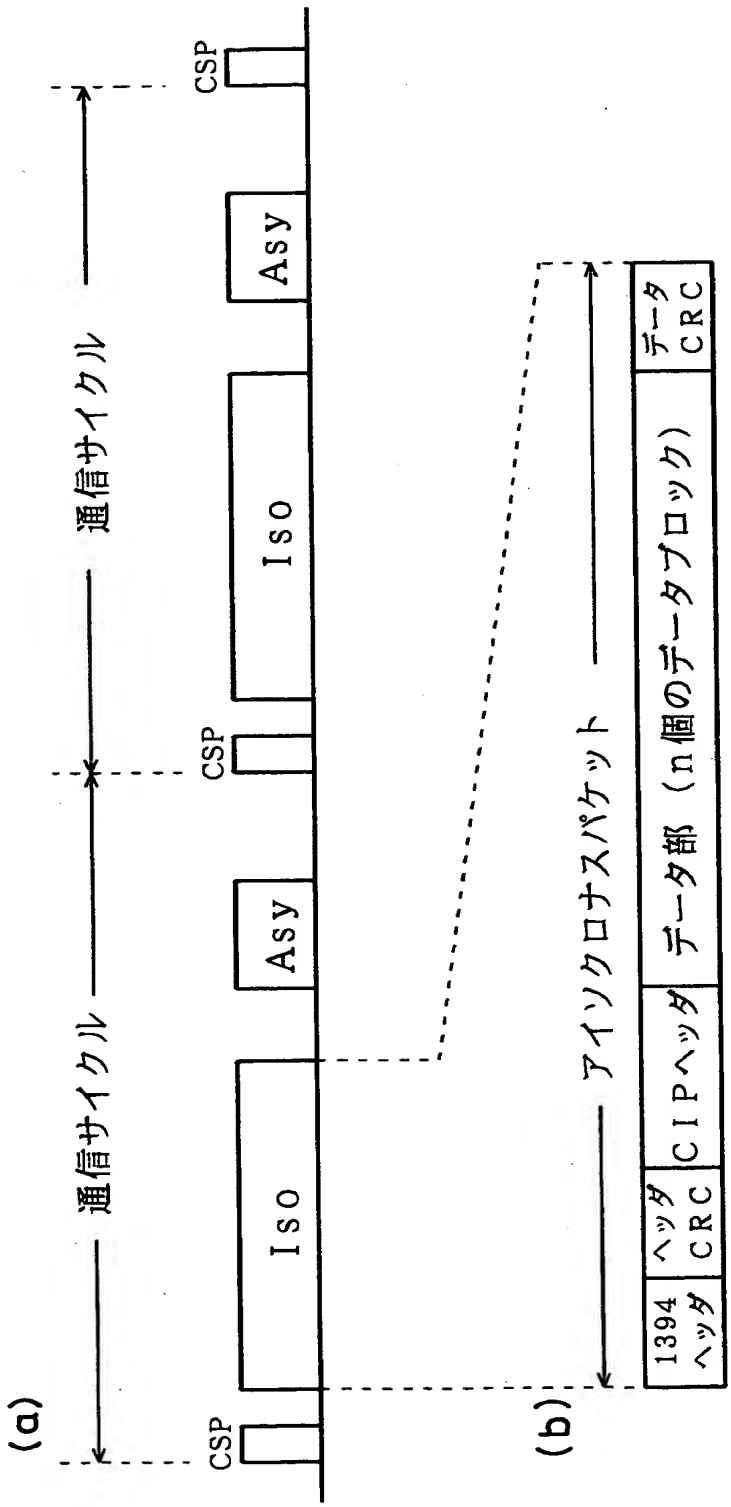
１　送信装置、２　受信装置、３　伝送路、４　記録装置、５　再生装置、６　メディア、１１，４１　ランダムデータ付加部、１２，４２　暗号化部、１３　送信部、２１　受信部、２２，５２　復号部、２３，５３　ランダムデータ除去部、４３　送出部、５１　取込部

【書類名】　　図面

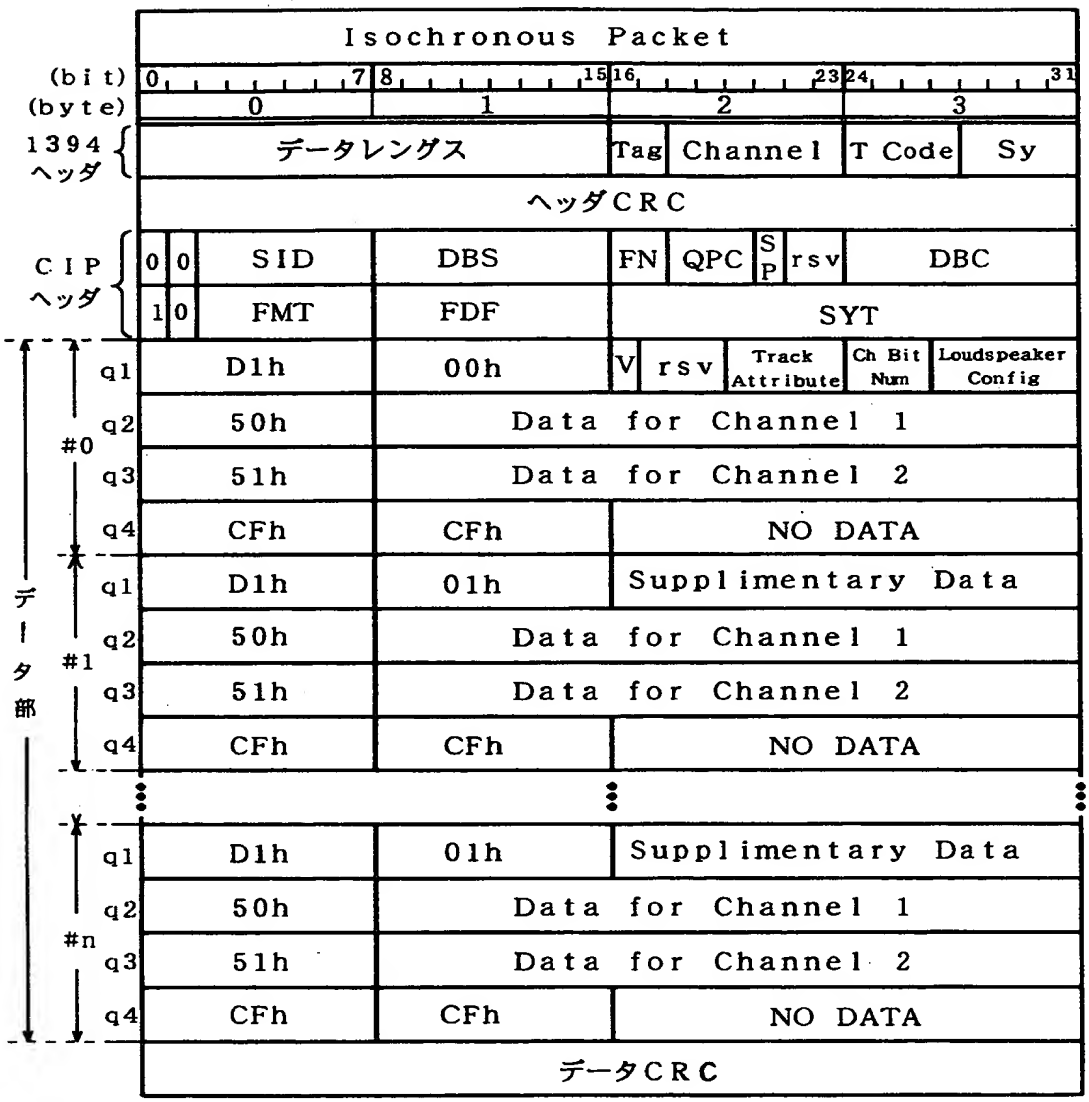
【図１】


データ
DT
ランダムデータ除去
23
DTad
復号
22
DTs
受信
21
2（受信装置）
3（伝送路）
DTs
解読不能
DT
（オールゼロ）
送信
13
DTs
暗号化
12
DTad
ランダムデータ付加
11
1（送信装置）
DT
データ

【図２】


(a)
通信サイクル
通信サイクル
CSP
Asy
Iso
CSP
Asy
Iso
CSP
(b)
アイソクロナスパケット
1394 ヘッダ
ヘッダ CRC
CIPヘッダ
データ部（n個のデータブロック）
データ CRC

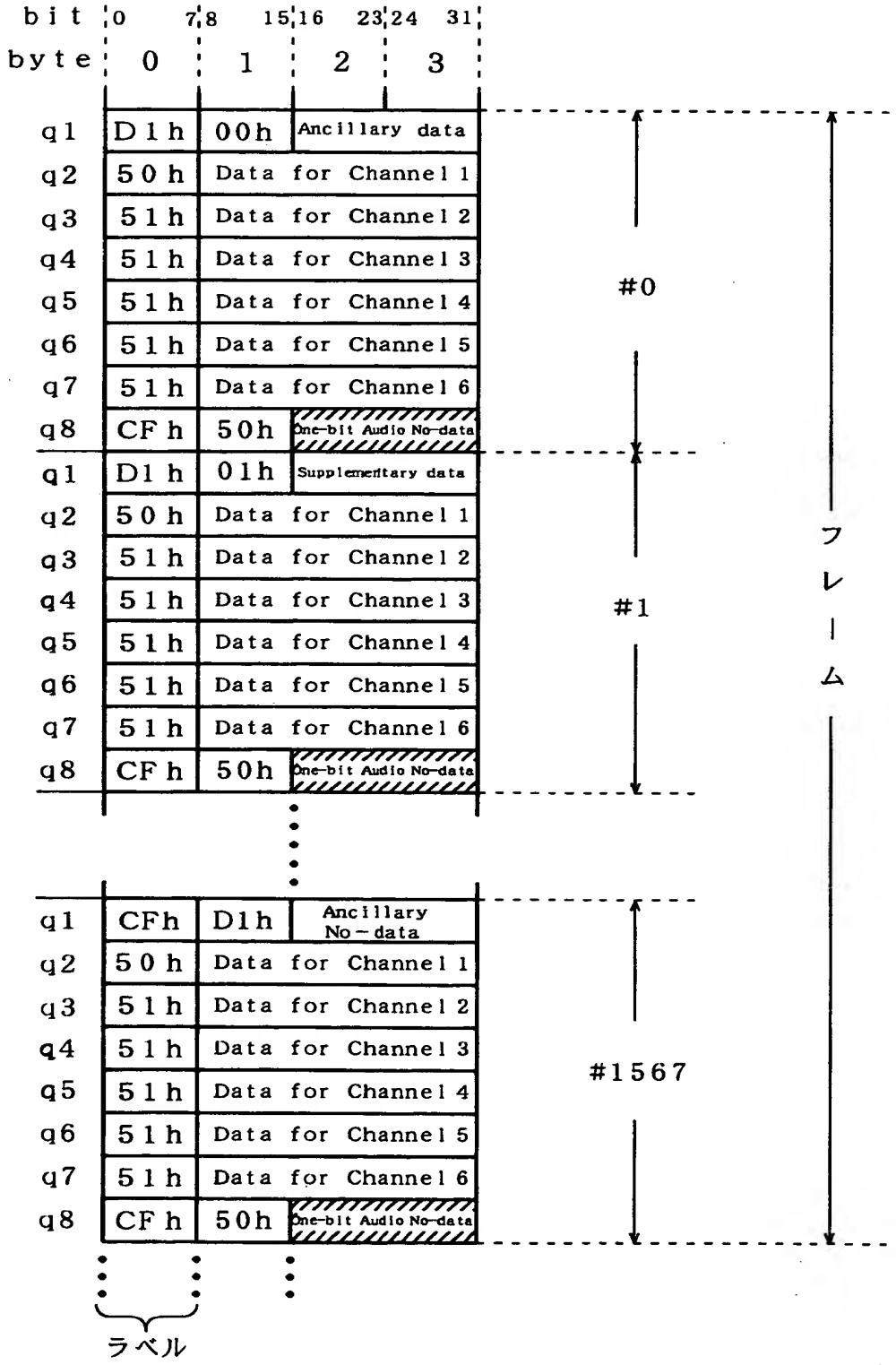
【図３】


Isochronous Packet
(bit)
(byte)
0
7
8
15
16
23
24
31
0
1
2
3
1394 ヘッダ
データレングス
Tag
Channel
T Code
Sy
ヘッダCRC
CIP ヘッダ
0
0
SID
DBS
FN
QPC
SP
rsv
DBC
1
0
FMT
FDF
SYT
データ部
#0
#1
#n
q1
q2
q3
q4
D1h
00h
V
rsv
Track Attribute
Ch Bit Num
Loudspeaker Config
50h
Data for Channel 1
51h
Data for Channel 2
CFh
NO DATA
01h
Supplimentary Data
データCRC

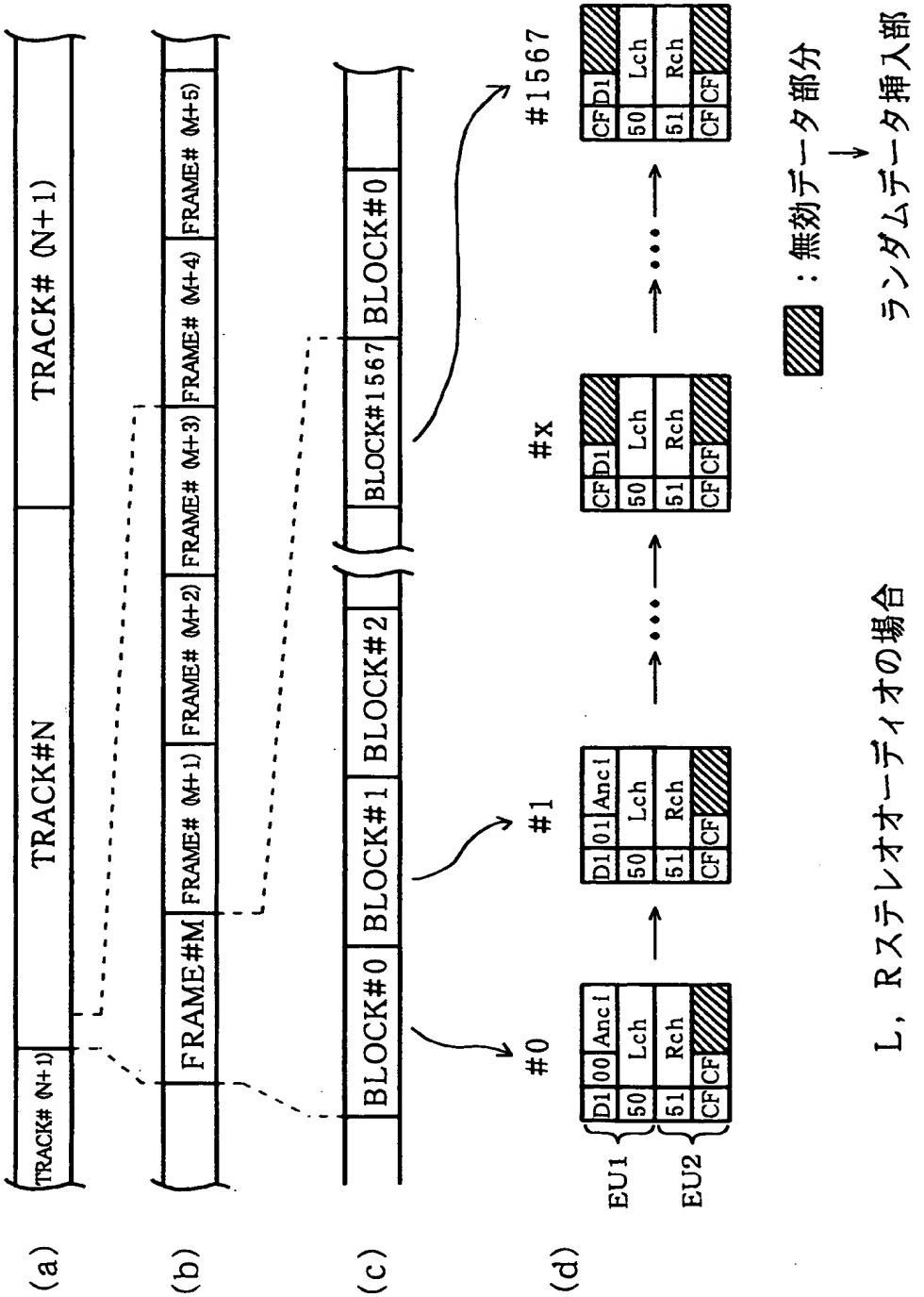
【図４】

Value	Description
00h-3Fh	IEC60958 Conformant
40h-4Fh	Multi-bit Linear Audio
50h-57h	One Bit Audio (Plain)
58h-5Fh	One Bit Audio (Encoded)
60h-7Fh	-reserved-
80h-83h	MIDI Conformant
84h-87h	Extended Music Data
88h-8Bh	SMPTE Time Code Conformant
8Ch-8Fh	Sample Count
90h-BFh	-reserved-
C0h-EFh	Ancillary Data
F0h-FFh	-reserved-

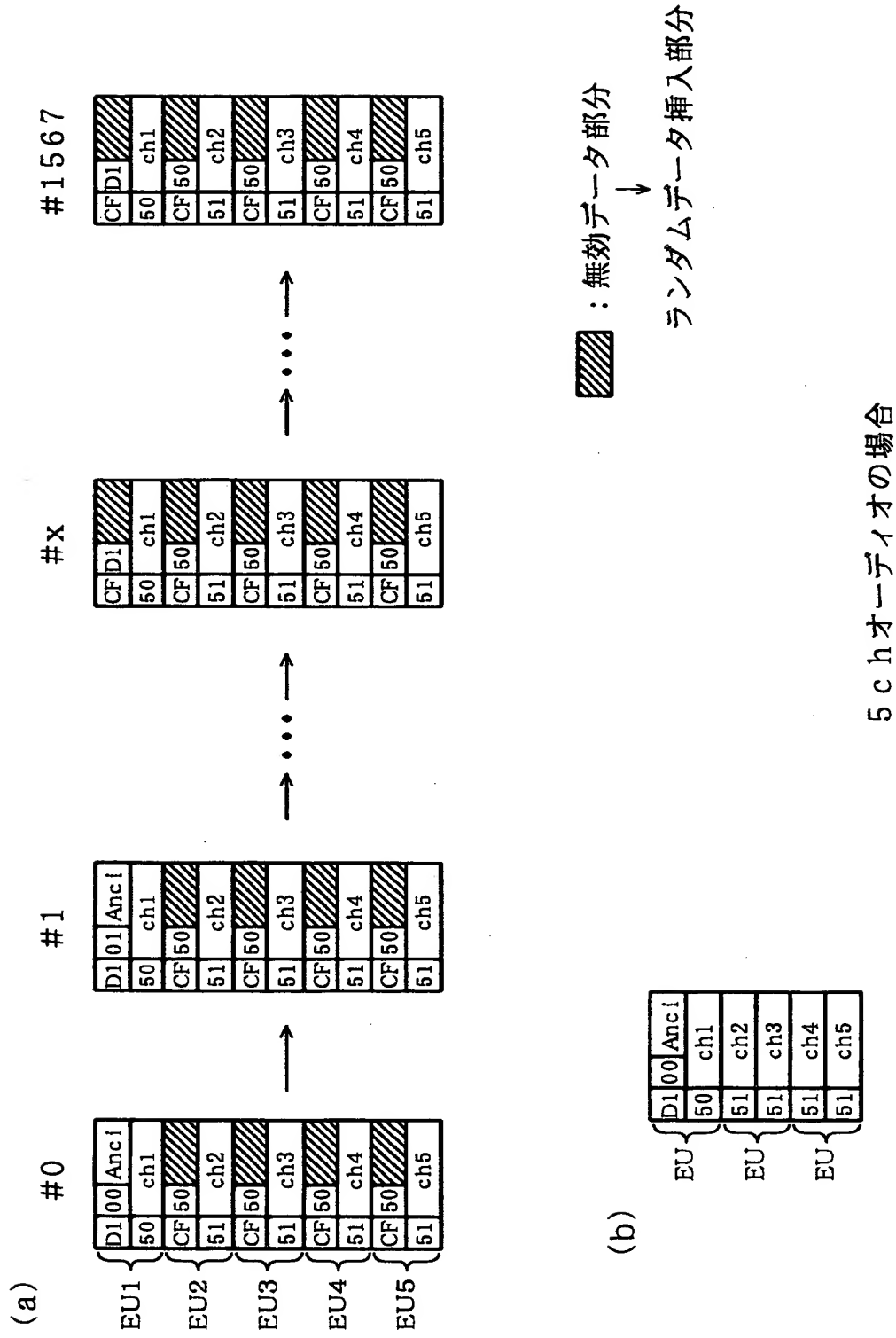
【図５】


bit
byte
0
7
8
15
16
23
24
31
0
1
2
3
q1
q2
q3
q4
q5
q6
q7
q8
D1h
00h
Ancillary data
50h
Data for Channel 1
51h
Data for Channel 2
Data for Channel 3
Data for Channel 4
Data for Channel 5
Data for Channel 6
CFh
One-bit Audio No-data
01h
Supplementary data
#0
#1
#1567
フレーム
Ancillary
No-data
ラベル

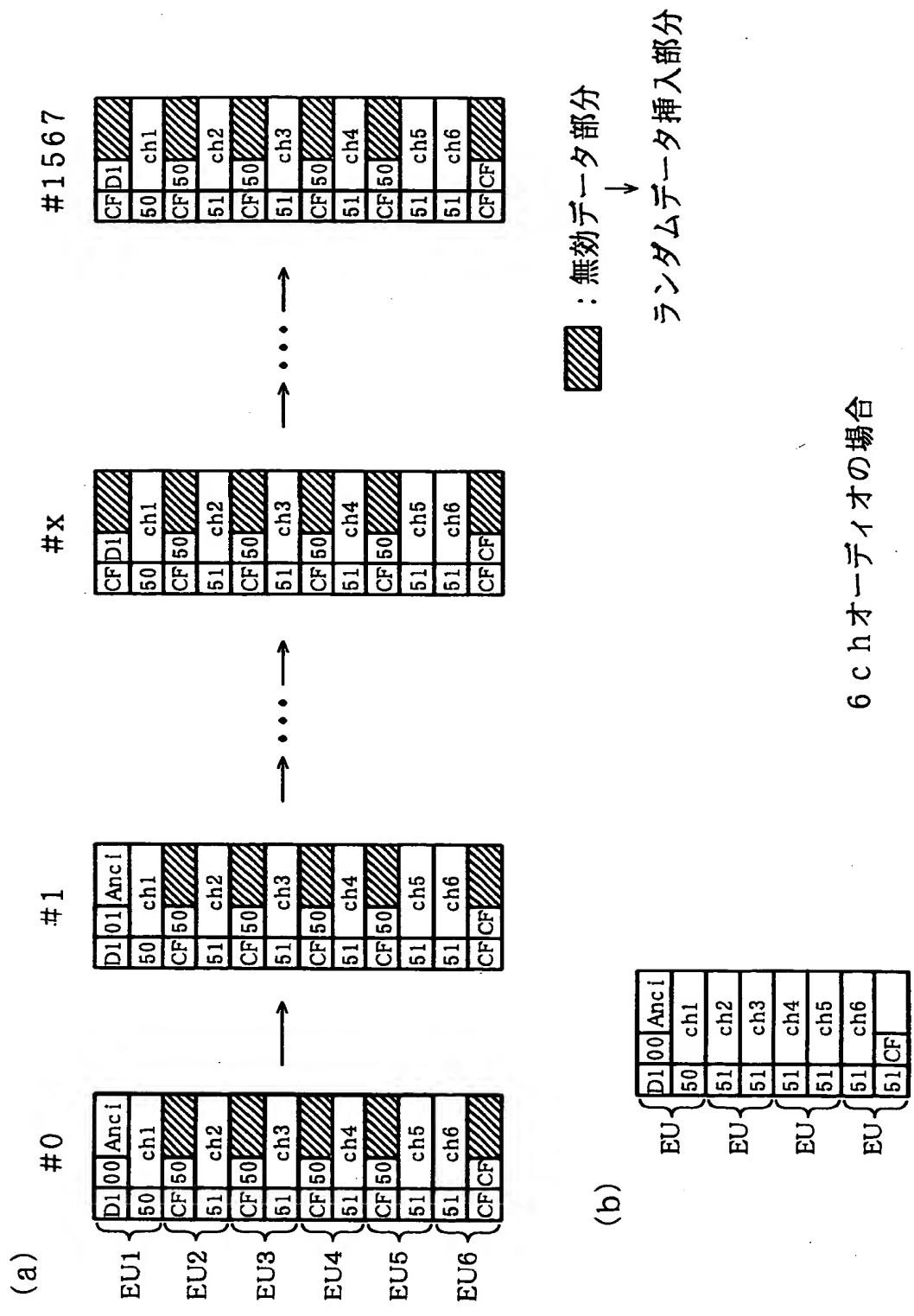
【図６】


(a)
TRACK#N
TRACK# (N+1)
TRACK# (N+1)
(b)
FRAME#M
FRAME# (M+1)
FRAME# (M+2)
FRAME# (M+3)
FRAME# (M+4)
FRAME# (M+5)
(c)
BLOCK#0
BLOCK#1
BLOCK#2
BLOCK#1567
BLOCK#0
(d)
#0
#1
#x
#1567
EU1
EU2
D1 00 Anc1
50 Lch
51 Rch
CF CF
D1 01 Anc1
CF D1
：無効データ部分
ランダムデータ挿入部
L，Rステレオオーディオの場合

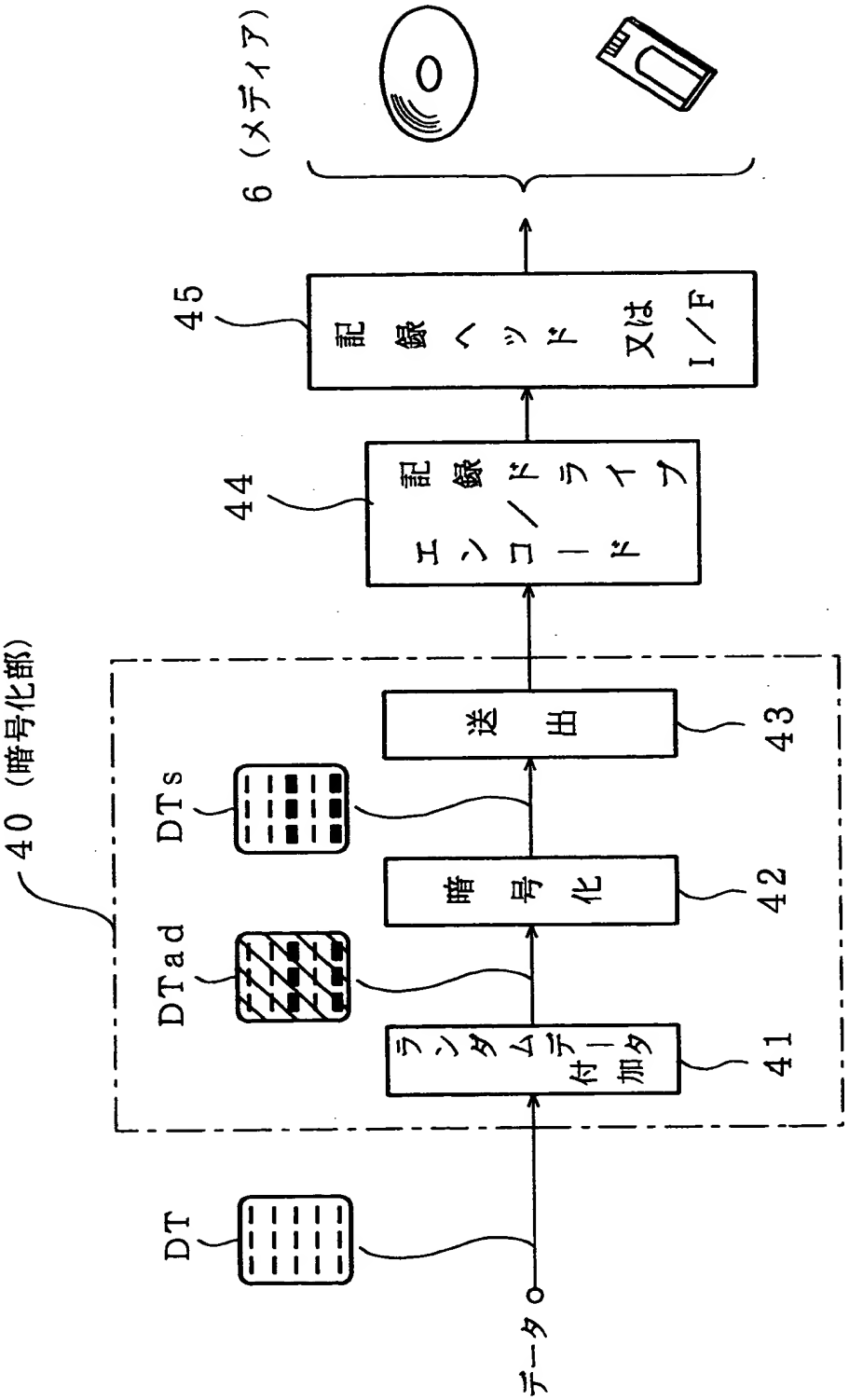
【図７】


(a)
#0
#1
#x
#1567
EU1
EU2
EU3
EU4
EU5
D1 00 Anc1
D1 01 Anc1
CF D1
50
CF 50
51
ch1
ch2
ch3
ch4
ch5
：無効データ部分
↓
ランダムデータ挿入部分
(b)
EU
EU
EU
5ｃｈオーディオの場合

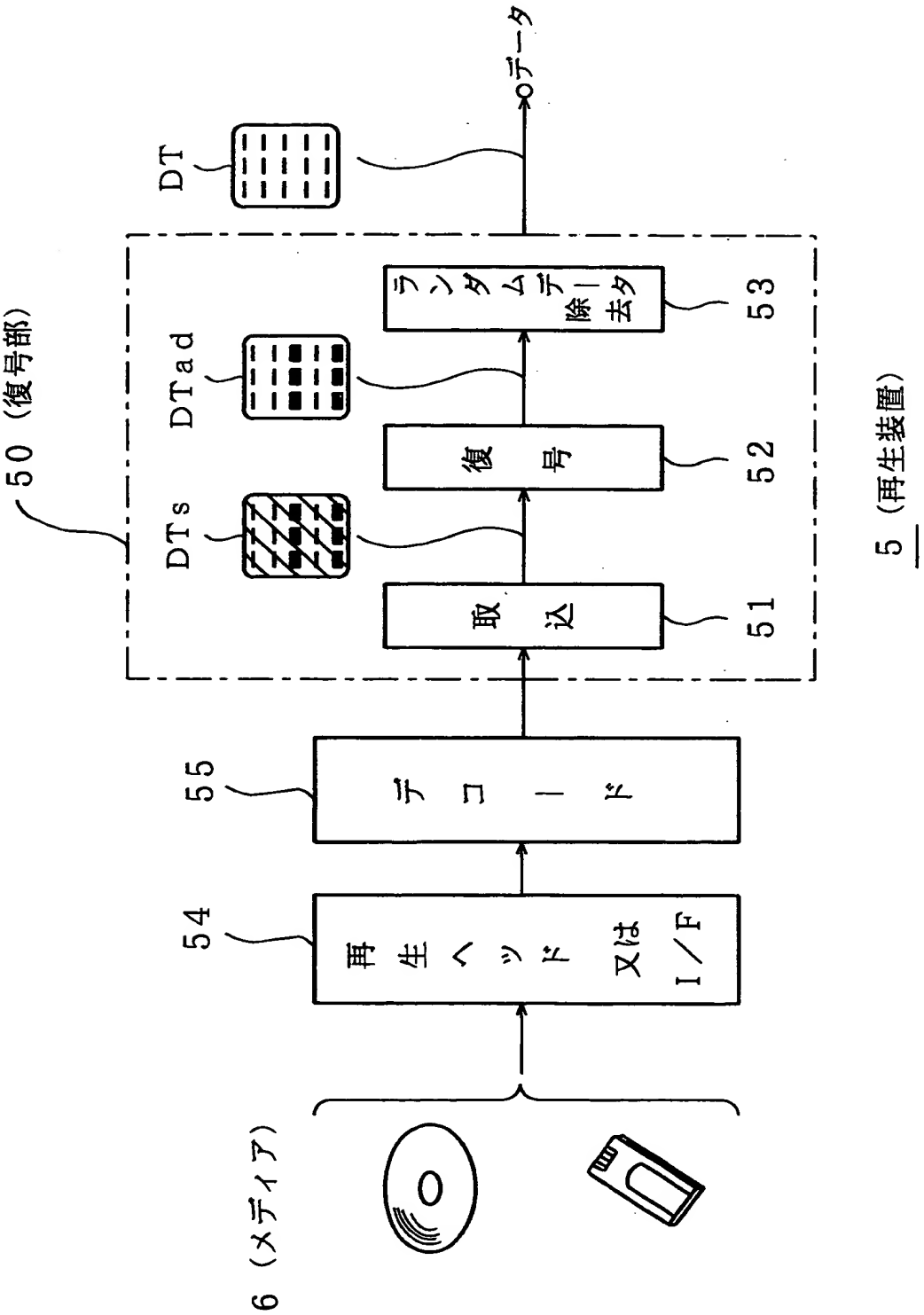
【図８】


(a)
#0
#1
#x
#1567
EU1
EU2
EU3
EU4
EU5
EU6
D1 00 Anci
D1 01 Anci
CF D1
50
51
CF 50
CF CF
ch1
ch2
ch3
ch4
ch5
ch6
：無効データ部分
ランダムデータ挿入部分
(b)
６ｃｈオーディオの場合

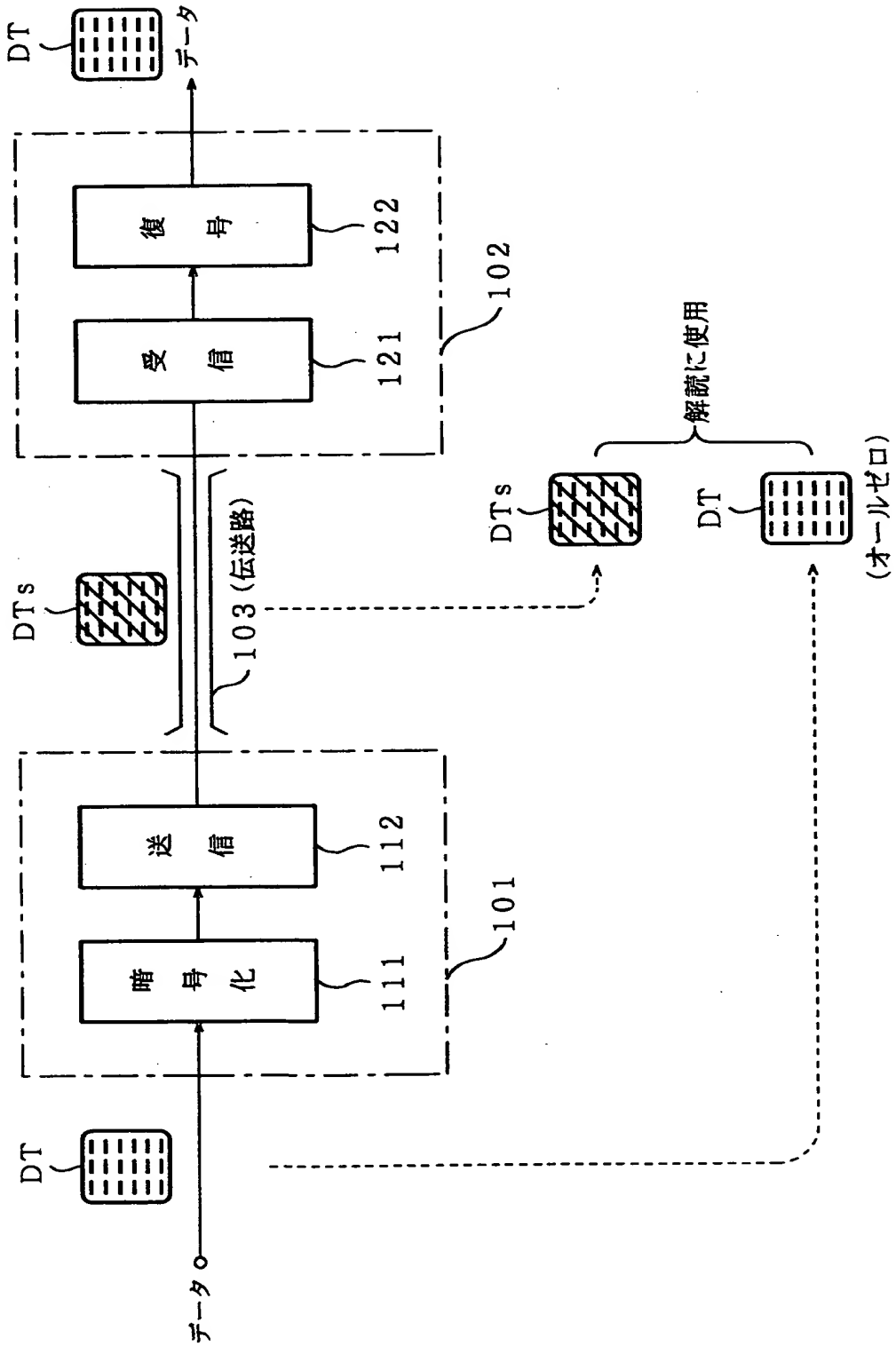
【図９】


6（メディア）
45
記録ヘッド又はI／F
44
記録ドライブエンコード
40（暗号化部）
DTs
DTad
DT
送出
暗号化
ランダムデータ付加
43
42
41
データ
4（記録装置）

【図１０】


6（メディア）
54
再生ヘッド又はI／F
55
デコード
50（復号部）
DTs
DTad
DT
取込
51
復号
52
ランダムデータ除去
53
データ
5（再生装置）

【図１１】


DT
データ
復号
122
受信
121
102
解読に使用
DTs
DT
(オールゼロ)
DTs
103(伝送路)
送信
112
暗号化
111
101
DT
データ

【書類名】　　要約書

【要約】

【課題】　暗号解読が困難で著作権保護などに好適なデータ伝送の実現。

【解決手段】　伝送するデータについて、パケットデータ内に乱数データを挿入したうえで暗号化を行なって伝送し、伝送過程などで暗号化データが抽出されたとしても、暗号アルゴリズムの解読を困難なものとする。データの復号は、暗号化を解読したうえで乱数データが挿入されたデータ部分を除去することで行う。また乱数データの挿入は暗号化処理の単位で行う。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－２５２８０４
受付番号	５００００１０６９５２１
書類名	特許願
担当官	高田　良彦　　２３１９
作成日	平成１２年　８月２９日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100086841
【住所又は居所】	東京都中央区新川１丁目２７番８号　新川大原ビル６階
【氏名又は名称】	脇　篤夫

【代理人】

【識別番号】	100114122
【住所又は居所】	東京都中央区新川１丁目２７番８号　新川大原ビル６階　脇特許事務所
【氏名又は名称】	鈴木　伸夫

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社